



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/999,766	07/23/1997	SCOTT A. MOSKOWITZ	2377/23	4344

29693 7590 04/05/2002

WILEY, REIN & FIELDING, LLP
ATTN: PATENT ADMINISTRATION
1776 K. STREET N.W.
WASHINGTON, DC 20006

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 04/05/2002

27

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

08/999,766

Applicant(s)

MOSKOWITZ ET AL.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 December 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 25-63 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 25-63 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s) _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other:

DETAILED ACTION

Response to Amendment

1. This action is in response to the comments filed 11 December 2001.

Response to Arguments

2. Applicant's arguments filed 11 December 2001 have been fully considered but they are not persuasive.
3. Elements not recited in the claims will not be read into the claims. As such, applicant's definition of a stega-cipher is not material to the claims. Nevertheless, three areas merit discussion: support for the definition, the initialization of the randomizer, and the similarities and differences between Powell et al. and the instant invention.
4. There is no support for the cipher function making use of potential data location information, a random or pseudo random seed, and the message data to generate a key, at least not in the sections cited by applicant in the communiqué under consideration. The examiner guesses that the only input into the generation of the key is the random or pseudo random seed.
5. Despite the section cited by applicant, the examiner remains skeptical that the output of the stega-cipher will differ even if all of the inputs are the same. This would imply that $f(c.d., m.d., k)$ will not equal another $f(c.d., m.d., k)$. This is possible, but only if f is a random function. And computers, such as those on which the instant invention would be running, do not perform random functions. If applicant will again allow the examiner to conjecture, it is possible that the statement cited in support of different outputs should be read in light of identical inputs being fed into a stega-cipher that has a

Art Unit: 2132

variable state. Thus the equation $f(c.d., m.d., k)$ should actually be $f(c.d., m.d., k, \text{internal state})$, where the internal state is updated with each use of the stega-cipher. Thus no two outputs of the same inputs would be the same (unless the internal state reverted to its original state – a highly unlikely proposition). The examiner considers the likelihood of an evolving internal state likely, primarily due to applicant's use of the word seed when referring to a random bit string; seed implies that the random value is operated upon repeatedly. In this case, the seed initializes the internal state; each time that a document is stega-ciphered, the internal state is altered. Thus, the actual equation performed by the stega-cipher is $f(c.d., m.d., \text{internal state}_i)$ where $\text{internal state}_i = f^i(k)$ where this nomenclature means f repeated i times. This might also explain the idea of the creation of a key, as proposed in applicant's description of the stega-cipher.

6. Applicant brings up three issues with respect to Powell et al.: lack of a cipher, lack of a key, and non-independence of watermark data. According to Webster's, a cipher is "a method of transforming a text in order to conceal its meaning." By this definition, Powell et al. use a cipher – the selection of insertion points and insertion constitute a method of transforming a text. The inserted material is hidden. Powell et al.'s use of a random choice of signature points reads on a key. Furthermore, the predetermined pattern could be argued to also read on a key, as could the storage of the bit value of each signature point together with x-y coordinates of the signature points. Of course, this last was clearly not used in the insertion of the watermark, but it does provide an interesting rebuttal to applicant's cogent contention that Powell et al. do

not teach a decoding key. Applicant's idea that Powell et al. does not teach watermarks is not as remarkable – the representation of the watermark depends on the environment, the content of the watermark does not. Hence the watermark is independent information, like applicant's invention.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 25-63 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. As has been discussed above, there is no teaching of using the watermark or potential data locations to form the key. The cited sections do not really show the random seed forming the key either, but this is readily believable.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

10. Claims 25, 27-29, 31-33, 35, 62, and 63 are rejected under 35 U.S.C. 102(a) as being anticipated by Bender et al. ("Techniques for data hiding").

In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be "invisible" or "inaudible", which meets the limitations of claims 62 and 63. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2, Bender is mentioned as encrypting the embedded data. A reading of the section cited as support for the amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but it is not quite entirely clear.

11. Claims 25-33, 35-39, 62, and 63 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Powell et al. (EPO 0 581 317 A2). See page 4, lines 4 and 40-42.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 34, 40-43, and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Schneier.

Powell et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

14. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Powell et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked

Art Unit: 2132

data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Powell et al. and Schneier's system.

15. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Powell et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Powell et al. and Schneier. Operating on only the start of message delimiter would hide data but decrease the reliability of authentication.

16. Claims 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Barton.

Powell et al. teach encrypting digital watermarks into information. They do not say that the watermarks are each unique. In lines 20-33 of column 4, Barton teaches including sequence data with authentication data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to

Art Unit: 2132

uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

17. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Barton as applied to claim 54 above.

Powell et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as verification. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

18. Claims 26, 30, and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Barton.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information includes a stream of digital samples. Barton's teaches embedding authentication information within a stream of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate digital sample streams as in Barton with the key-encrypted watermarks of Bender et al.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that each sample has unique watermark information. In lines 20-33 of

column 4, Barton teaches including sequence data with the authentication data. The authentication data is a reduced representation of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

Pre-processing sample windows is inherent, as is determining which and how many windows will contain watermark information.

19. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information is then modified. Encryption modifies data. Official notice is taken that encrypting information in order to protect the data from unauthorized viewing is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it.

20. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Morris.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that one bit is read out of every sample for the watermark. In lines 50-52 of the third column, Morris says that the human ear cannot detect the difference between a sound value of 64000 and 64001. This would be a one-bit change of the least significant bit. As taught by Morris, these small changes can be used to carry

identification codes. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to discretely carry the watermark information of Bender et al. in the least significant bits as taught by Morris.

21. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Powell et al. (5930377).

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that samples are mapped to extract bits of information. As is explained in their abstract and diagrams, Powell et al. teach a method of embedding a digital watermark which requires use of a map of an image to determine the places to embed the watermark. This method is advantageous because, as explained in lines 42-43 of column 1, it is resistant to image modification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the mapping techniques of Powell to the encryption system of Bender et al. so as to make the data's watermark resistant to data modification.

22. Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Braudaway et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not set out that the watermark is used in any specific manner.

By watermarking the data, Braudaway et al.'s method creates a first derivative encoded signal. It is inherent that attempts to decode the watermark without the proper key would further obfuscate the information. It was once theorized that encrypting information with two keys in order to strengthen security could in fact be mimicked by

using one key that would possibly be easier to break. Although this theory has since been proven incorrect, the immediate solution was to strengthen security by encrypting with a first key and then decrypting with a non-corresponding second key. Providing information is inherent.

In the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark. This change in brightness anticipates claim 38's spectral values. Also in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark. These non-transparent values form a map to meet claim 39.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate any of the teachings of Braudaway into Bender et al. 23. Claims 40-43 and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Schneier.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This

Art Unit: 2132

anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

24. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Bender et al. and Schneier's system.

25. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Bender et al. and Schneier.

26. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Barton as applied to claim 54 above.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as a verification. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

Conclusion

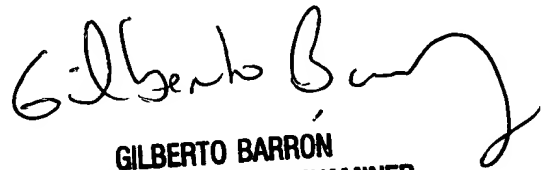
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O. Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
April 2, 2002


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100